SHAREPOINT

Microsoft 365 Backup: Wiederherstellungsfenster für SharePoint und OneDrive bis 10 Jahre

Consulting Briefing · 28.11.2026 · boddenberg.de

Executive Summary

Microsoft hat das Gedächtnis seines Backups verfünffacht, und niemand ist gezwungen, es zu benutzen. Laut Microsoft-Ankündigung MC1567262 kannst du in Microsoft 365 Backup für SharePoint-Sites und OneDrive-Konten jetzt Wiederherstellungsfenster von bis zu zehn Jahren einstellen. Bisher war bei zwei Jahren Schluss. Die Funktion ist weltweit allgemein verfügbar, es gibt keine Frist, keine Abkündigung und keine automatische Umstellung: Der Standard bleibt bei einem Jahr, Exchange bleibt bei maximal zwei Jahren.

Technisch ist das ein Schieberegler. Organisatorisch ist es eine Grundsatzfrage. Wer das Fenster aufzieht, bewahrt personenbezogene Daten deutlich länger auf, auch solche, die im Livesystem längst nach Löschkonzept entsorgt wurden. Das berührt den Grundsatz der Speicherbegrenzung aus Art. 5 DSGVO, das Verzeichnis der Verarbeitungstätigkeiten, die Datenschutzhinweise für die Belegschaft und in vielen Häusern die Betriebs- oder Dienstvereinbarung zu Microsoft 365. Unsere Empfehlung: Nichts überstürzen, Bedarf je Site begründen, und erst dann klicken.

Fakten: Das Wichtigste auf einen Blick

Quelle: Microsoft-Ankündigung MC1567262, zuletzt geändert am 24.11.2026. Betroffen: Microsoft 365 Backup, SharePoint Online, OneDrive for Business.

Neu: Fenster von 3 und 6 Monaten sowie 1 bis 10 Jahren für SharePoint- und OneDrive-Richtlinien. Exchange bleibt bei 3 Monaten, 6 Monaten, 1 oder 2 Jahren.

Standard: unverändert ein Jahr. Längere Fenster stellst du pro Richtlinie ein, rückwirkend entsteht keine ältere Historie.

Handlungsbedarf: keiner, solange du nichts änderst. Dringlichkeit: niedrig, Klärung mit Datenschutz bis Ende Q1 2027 sinnvoll.

Worum geht es im Detail?

Kurz zur Einordnung, was Microsoft 365 Backup eigentlich ist. Es ist Microsofts eigener Backup-Dienst innerhalb der Microsoft-365-Vertrauensgrenze, abgerechnet nach Verbrauch: laut Microsoft Learn 0,15 US-Dollar pro GB geschützter Inhalte und Monat, Wiederherstellungen sind kostenlos. Die Daten verlassen die Geo-Region deines Mandanten nicht, und die Sicherungen liegen in einem Append-only-Speicher. Purview-Aufbewahrungs- und Löschrichtlinien wirken ausdrücklich nicht darauf. Das ist gewollt, denn ein Backup, das ein kompromittierter Admin per Löschrichtlinie leerräumen kann, ist eher eine Leihgabe.

Die Wiederherstellungspunkte sind nicht gleichmäßig verteilt. In den ersten 14 Tagen gibt es für SharePoint und OneDrive Punkte im 10-Minuten-Takt, und nur in diesem Zeitraum kannst du

einzelne Dateien und Ordner zurückholen. Danach bleibt ein Punkt pro Woche, und mit diesem kannst du nur noch die komplette Site oder das komplette OneDrive-Konto wiederherstellen, entweder an Ort und Stelle oder unter einer neuen URL. Das Fenster bestimmt, wie lange diese Wochenpunkte stehen bleiben. Bisher war nach spätestens zwei Jahren Schluss, jetzt nach bis zu zehn.

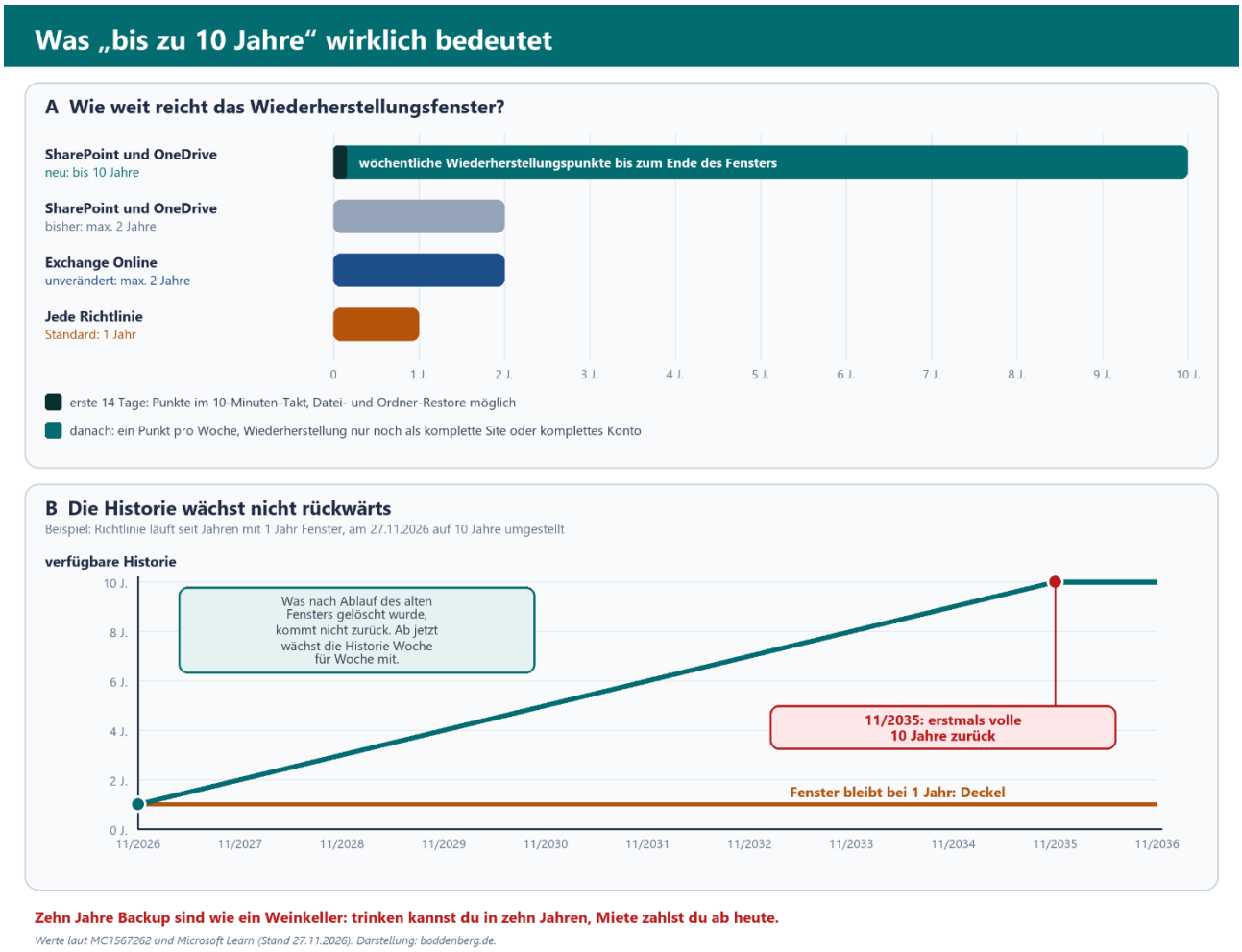

Abbildung 1: Das neue Fenster reicht weit, aber nur grob, und die Historie wächst erst ab der Umstellung.

Der Haken steht im Kleingedruckten: Die Zeitmaschine fährt nur vorwärts. Wer heute auf zehn Jahre stellt, hat morgen nicht zehn Jahre Historie. Alles, was nach Ablauf des alten Fensters gelöscht wurde, ist weg. Ab der Umstellung bleiben die Wochenpunkte einfach länger liegen, und die volle Dekade hast du frühestens 2035 oder 2036 beisammen. Umgekehrt gilt laut Microsoft Learn: Verkürzt du ein Fenster, werden ältere Punkte nach einer Karenzzeit von 30 Tagen gelöscht. Das ist die eingebaute Bedenkzeit, bevor ein Fehlklick Jahre an Sicherungen verdampfen lässt.

Und warum macht Microsoft das? Weil Drittanbieter wie Veeam, AvePoint oder Commvault seit Jahren mit langen oder unbegrenzten Aufbewahrungszeiten werben und Microsoft in Ausschreibungen genau daran gemessen wird. Dazu kommen Branchen, in denen Prüfer gern fragen, ob man den Stand einer Projektablage von vor fünf Jahren rekonstruieren kann. Mit zehn Jahren hat Microsoft diese Lücke im Datenblatt geschlossen, wobei das Feature deutlich mehr Häkchen in der Vergleichstabelle als Nutzen im Alltag erzeugt.

Merkmal	SharePoint und OneDrive	Exchange Online
Wählbare Fenster	3 Monate, 6 Monate, 1 bis 10 Jahre	3 Monate, 6 Monate, 1 Jahr, 2 Jahre
Standard	1 Jahr	1 Jahr
Feingranulare Wiederherstellung	Dateien und Ordner, nur letzte 14 Tage	Elemente wie Mails und Termine
Punkte nach 14 Tagen	wöchentlich, nur komplette Site oder Konto	10-Minuten-Takt über 52 Wochen
Fenster verlängern	sofort wirksam, keine rückwirkende Historie	nur bis 2 Jahre
Fenster verkürzen	ältere Punkte fallen nach 30 Tagen Karenz weg	ebenso

Was sind Chancen? Was sind Risiken?

Die Chance: Schäden, die keiner rechtzeitig bemerkt. Ransomware fällt meist schnell auf, weil plötzlich jemand schreiend im Flur steht. Gefährlicher ist der schleichende Schaden. Ein Maschinenbauer aus unserer Beratungspraxis hatte eine Projektsite, auf der ein falsch konfigurierter Sync-Client über Monate Dateien durch ältere Fassungen ersetzte. Aufgefallen ist es nach 17 Monaten, als ein Kunde die Konstruktionsstände eines reklamierten Bauteils sehen wollte. Mit einem Jahr Fenster lautet die Antwort in so einem Fall: „Tja." Mit drei Jahren hätte man die Site unter einer neuen URL wiederhergestellt und die richtigen Stände herausgefischt. Für solche Projektablagen, Konstruktionsdaten und Gutachten ist ein längeres Fenster ein echter Gewinn.

Das Risiko: Dein Löschkonzept bekommt einen Zwilling, der nichts vergisst. Nehmen wir eine Stadtverwaltung, die Bewerbungsunterlagen in einer SharePoint-Site ablegt und nach sechs Monaten per Purview-Richtlinie sauber löscht. Steht dieselbe Site in einer Backup-Richtlinie mit zehn Jahren Fenster, liegen die Unterlagen der abgelehnten Kandidaten im Wochenpunkt weiter, technisch völlig korrekt und rechtlich schwer zu erklären. Das Backup ist bewusst von Purview isoliert. Was die Ransomware-Abwehr stark macht, macht den Datenschutz schwach.

> **Warnung: Das Backup ist kein Archiv, auch wenn es sich so anfühlt**
>
> Der Klassiker in jeder zweiten Kanzlei: „Wir müssen zehn Jahre aufbewahren, jetzt kann das Backup zehn Jahre, Problem gelöst." Nein. Die steuerliche Aufbewahrung verlangt, dass du einzelne Belege findest, lesbar machst und nach Fristablauf gezielt entsorgst. Ein Wochenpunkt kann nur die ganze Site zurückspielen, kennt keine Frist pro Dokument und lässt sich nicht pro Beleg löschen. Wer damit vor dem Betriebsprüfer steht, restauriert vor dessen Augen eine Site aus dem Jahr 2029 und hofft, dass der Kaffee lange reicht.

Datenschutz: drei Pflichten, die mit dem Schieberegler wach werden. Erstens brauchst du für die Verlängerung einen dokumentierten Zweck und eine tragfähige Rechtsgrundlage.

Datensicherung ist als berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DSGVO bzw. als Teil der Sicherheit der Verarbeitung nach Art. 32 anerkannt, aber nur in der Länge, die der Zweck trägt. „Weil es geht“ ist kein Zweck. Zweitens musst du die Speicherdauer im Verzeichnis der Verarbeitungstätigkeiten und in den Datenschutzhinweisen für die Belegschaft anpassen, denn Art. 13 verlangt Angaben zur Speicherdauer. Drittens kommt das Löschrecht aus Art. 17: Laut Microsoft Learn löschst du Backups nur pro Site, Konto oder Postfach über das Offboarding, mit 90 Tagen Karenzzeit oder sieben Tagen bei Freigabe durch einen zweiten Administrator. Einzelne Dateien lassen sich nicht aus der Sicherung entfernen.

Die Aufsichtsbehörden akzeptieren in der Praxis, dass Backups nicht selektiv bereinigt werden, wenn sie in einem festen Zyklus auslaufen und gelöschte Daten bei einer Wiederherstellung sofort erneut gelöscht werden. Dieses Argument wird mit jedem zusätzlichen Jahr dünner. Bei sechs Monaten Restlaufzeit nickt der Datenschutzbeauftragte, bei neun Jahren greift er zum Telefon. Für Sites mit Personalakten, Gesundheits- oder Sozialdaten gehört ein langes Fenster deshalb in eine Datenschutz-Folgenabschätzung oder zumindest in die Aktualisierung der bestehenden.

Mitbestimmung und Lizenzen. Ein Backup ist keine Überwachungseinrichtung, aber wer OneDrive-Konten zehn Jahre sichert, kann theoretisch rekonstruieren, wer wann welche Datei hatte. Viele Betriebsvereinbarungen zu Microsoft 365 regeln Speicher- und Löschfristen ausdrücklich, und die gelten dann auch für die Sicherung. Im öffentlichen Dienst kommt der Personalrat dazu, außerdem die Frage nach der Anbietungspflicht gegenüber dem zuständigen Archiv: Was im Backup liegt, ist dem Archiv nicht angeboten worden. Lizenzrechtlich ist das Feature unspektakulär: Der Preis pro GB hängt nicht von der Fensterlänge ab. Teurer wird es indirekt, weil gelöschte und versionierte Inhalte laut Microsoft Learn bis zum Ablauf des Fensters mitberechnet werden. Du zahlst also unter Umständen zehn Jahre Miete für Dateien, die schon lange niemand mehr will.

Aspekt	Chance	Risiko	Gewicht
Betrieb	Rettung bei spät entdeckten Schäden, Rekonstruktion alter Projektstände	grobe Wochenpunkte, nur Komplett-Restore, erst ab Umstellung verfügbar	mittel
Datenschutz	dokumentierter, begründeter Sicherungszweck	Speicherbegrenzung, Löschkonzept wird ausgehebelt, Art. 17 nur pro Site	hoch
Mitbestimmung	Anlass, Sicherungsfristen sauber zu regeln	Verstoß gegen vereinbarte Löschfristen	mittel
Kosten	kein Aufpreis für das Fenster selbst	gelöschte Inhalte bleiben jahrelang abrechnungsrelevant	mittel
Compliance	Nachweis früherer Stände gegenüber Kunden und Prüfern	Verwechslung mit Archivierung und gesetzlicher Aufbewahrung	hoch

Was müssen wir jetzt schon vorbereiten?

Gute Nachricht zuerst: Nichts brennt. Microsoft schreibt selbst, dass keine Aktion nötig ist, wenn du die aktuellen Fenster behalten willst. Die schlechte Nachricht: Jeder Backup-Admin kann ab

sofort eine Richtlinie auf zehn Jahre ziehen, und außer dem Audit-Log merkt es niemand. Der wichtigste Schritt ist deshalb kein technischer, sondern eine Regel, wer das darf und wann.

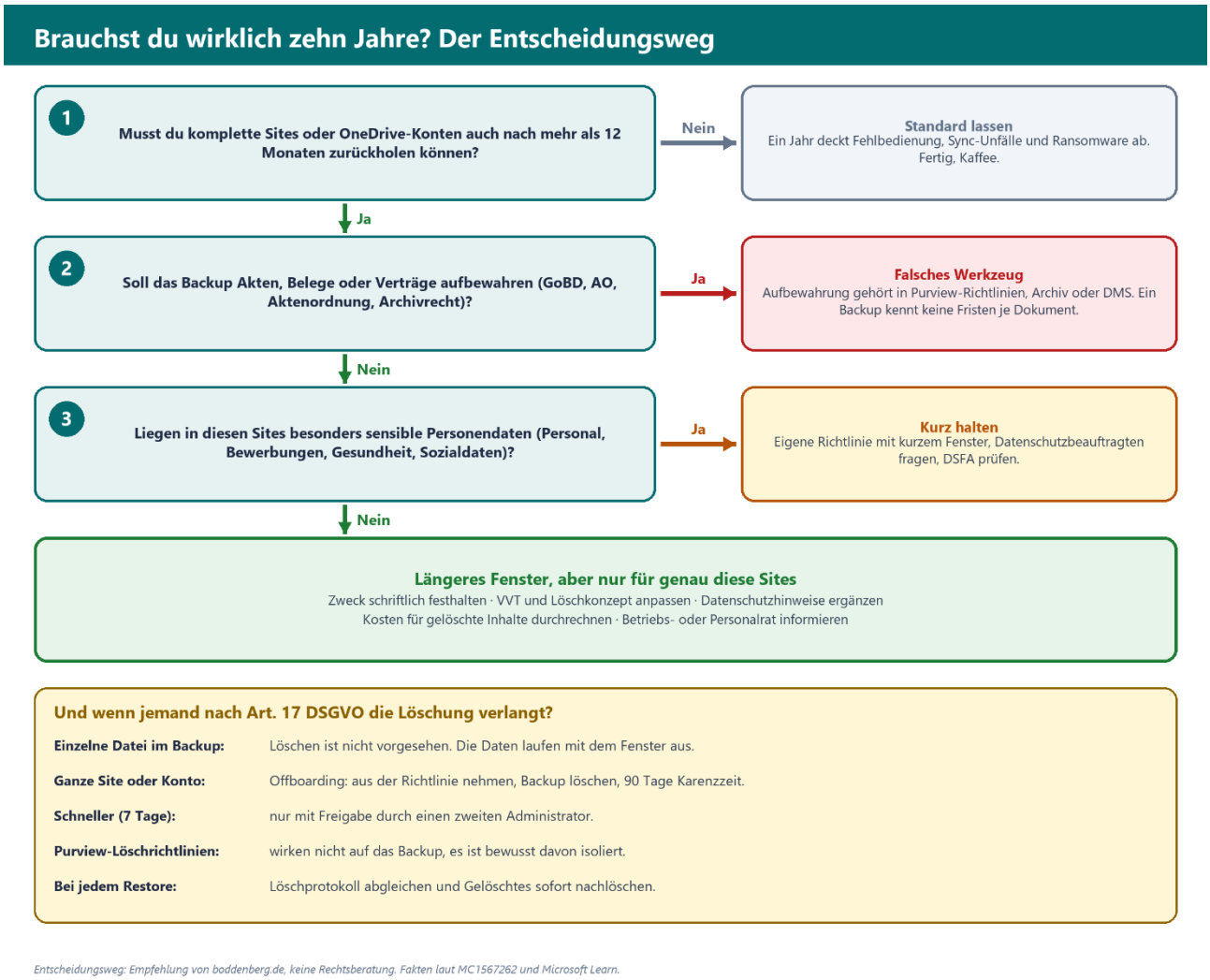

Abbildung 2: Vom Wunsch nach zehn Jahren bleibt nach drei ehrlichen Fragen meist eine kleine, begründete Gruppe von Sites übrig.

Tipp: Richtlinien nach Schutzbedarf schneiden, nicht nach Bequemlichkeit

Eine Site, ein Konto oder ein Postfach kann laut Microsoft Learn nur in genau einer Richtlinie stehen. Bau dir deshalb mehrere SharePoint-Richtlinien: eine Standardrichtlinie mit einem Jahr, eine Langzeitrichtlinie für Projekt- und Konstruktionsablagen und eine kurze für Personal- und Bewerbersites.

Den Weg findest du im Microsoft 365 Admin Center unter Einstellungen › Microsoft 365 Backup: Richtlinie öffnen, auf der Seite der Sicherungseinstellungen das Wiederherstellungsfenster wählen und mit „Richtlinie aktualisieren“ speichern. Pausierte Richtlinien und laufende Sicherungen lassen sich nicht ändern.

Wann	Wer	Was konkret
Bis 12.12.2026	Backup-Admin	Bestehende Richtlinien und Fenster dokumentieren. Klären, wer Backup-Richtlinien ändern darf, Änderungen im Audit-Log überwachen.
Bis 18.12.2026	IT-Leitung	Regel festlegen: keine Verlängerung über ein Jahr ohne Freigabe durch Datenschutz und Fachbereich.
Januar 2027	Fachbereiche, Backup-Admin	Sites mit echtem Langzeitbedarf benennen, Zweck je Site begründen, Kosten mit dem Rechner von Microsoft abschätzen.
Bis 28.02.2027	Datenschutzbeauftragter	VVT, Löschkonzept und Datenschutzhinweise ergänzen, DSFA für sensible Sites prüfen, Nachlöschprozess für Restores festschreiben.
Bis 31.03.2027	IT-Leitung, Gremium	Betriebs- oder Personalrat informieren, Vereinbarung um Sicherungsfristen ergänzen, danach Langzeitrichtlinie aktivieren.
Jährlich	Backup-Admin, DSB	Fenster und Kosten überprüfen, nicht mehr benötigte Sites über das Offboarding aus der Sicherung nehmen.

Wichtig: Kommunikation an die Belegschaft: sachlich, kurz, ehrlich

Eine Rundmail „Wir speichern jetzt alles zehn Jahre“ erzeugt genau die Panik, die du nicht willst, und ist meistens auch falsch. Ergänze stattdessen die Datenschutzhinweise und das Intranet um einen Absatz: Welche Bereiche wie lange gesichert werden, wozu, und dass gelöschte Inhalte im Backup nicht wieder auftauchen, ohne dass sie erneut gelöscht werden. Wer das sauber formuliert, beantwortet die nächste Auskunftsanfrage nach Art. 15 in zehn Minuten statt in zehn Tagen.

Die Einstellmöglichkeiten beschreibt Microsoft im Learn-Artikel Erstellen, Anzeigen und Bearbeiten von Sicherungsrichtlinien in Microsoft 365 Backup, das Löschen einzelner Sicherungen im Artikel Offboarding von Microsoft 365 Backup.

Weiterlesen auf boddenberg.de

› Microsoft 365 Backup: Full Workload Backup für SharePoint, OneDrive und Exchange
› Backup und Wiederherstellung in Microsoft 365: Die Risikoentscheidung fürs Rechnungsprüfungsamt
› Aufbewahrung und Aussonderung mit Purview: Fristen, Disposition, Vernichtungsnachweis
› Purview Priority Cleanup löscht OneDrive- und SharePoint-Inhalte endgültig

Häufig gestellte Fragen

Wie lange kann Microsoft 365 Backup SharePoint und OneDrive maximal sichern?

Laut Microsoft-Ankündigung MC1567262 sind für SharePoint-Sites und OneDrive-Konten Wiederherstellungsfenster von bis zu zehn Jahren möglich, wählbar in Jahresschritten. Der Standard bleibt bei einem Jahr, Exchange-Postfächer lassen sich weiterhin höchstens zwei Jahre zurück wiederherstellen.

Habe ich nach der Umstellung auf zehn Jahre sofort Zugriff auf ältere Sicherungen?

Nein, eine Verlängerung erzeugt keine älteren Wiederherstellungspunkte. Die Historie wächst ab der Umstellung Woche für Woche mit, die vollen zehn Jahre stehen also erst rund zehn Jahre nach Aktivierung des Schutzes bereit.

Kann ich mit Microsoft 365 Backup einzelne Dateien von vor drei Jahren wiederherstellen?

Nicht direkt, denn einzelne Dateien und Ordner lassen sich nur aus den letzten 14 Tagen zurückholen. Ältere Wochenpunkte stellen nur die komplette Site oder das komplette OneDrive-Konto wieder her, am besten unter einer neuen URL, aus der du die gesuchte Datei anschließend herauskopierst.

Kostet ein längeres Wiederherstellungsfenster in Microsoft 365 Backup mehr?

Der Preis von 0,15 US-Dollar pro GB geschützter Daten und Monat hängt nicht von der Fensterlänge ab. Gelöschte und versionierte Inhalte werden aber bis zum Ablauf des Fensters mitberechnet, weshalb ein langes Fenster die Rechnung indirekt erhöhen kann.

Ist eine zehnjährige Backup-Aufbewahrung mit der DSGVO vereinbar?

Das ist möglich, wenn ein konkreter Sicherungszweck die Dauer trägt und Verzeichnis der Verarbeitungstätigkeiten, Löschkonzept und Datenschutzhinweise angepasst sind. Weil sich einzelne Dateien nicht aus dem Backup löschen lassen, sollten Sites mit sensiblen Personendaten kurze Fenster behalten und Wiederherstellungen immer mit einem Nachlöschprozess verbunden sein.